Zero Trust Implementation Lessons Learned

Zero Trust is simultaneously a concept, a framework, an approach, an architecture, a set of guiding principles, a systems design, and an operational model to cybersecurity and risk management.

Joseph Klimavicz
Managing Director
KPMG LLP

Today, every government agency is completely dependent on digital technology to perform its mission, and everyone is counting on Zero Trust to secure this technology and associated data to ensure citizen services and national security. The Executive Order (EO) 14028 on Improving the Nation's Cybersecurity (May 12, 2021) emphasized Zero Trust, but what are some of the big lessons learned implementing Zero Trust?

Zero Trust is simultaneously a concept, a framework, an approach, an architecture, a set of guiding principles, a systems design, and an operational model to cybersecurity and risk management that safeguards the environment no matter where data and people reside to build the capability to trust nothing and verify everything.

This broad definition of success means some government agencies may have already claimed victory, but in my federal service experiences as well as recent experiences supporting federal clients, the reality is a few government agencies have limited Zero Trust implementations. Sharing Zero Trust lessons learned from these early implementations will be critical to broader rollout across the federal landscape.

With Zero Trust, the user's identity, their devices, the software, the network, or the data could be compromised, and agencies need to implement Zero Trust controls across these six foundational elements: identities, devices, applications, data, infrastructure, and networks.

This approach ensures that identities are verified and authenticated and that devices are compliant before granting access to any resources. Visibility and analytics, along with automation, need to be applied continually and comprehensively. Zero Trust implementations requires significant integration of third-party applications, but agencies can leverage key cyber services from the big cloud service providers to streamline implementation.

Zero Trust may seem like a lot to take on, however, the use of existing technologies and revamping of current processes and strategies can allow agencies to implement a new approach to cybersecurity without huge capital investments. Government agencies may already have many of the components in place providing many of the alerts and analysis needed for Zero Trust. For example, existing Identity, Cre-

With Zero Trust, the user's identity, their devices, the software, the network, or the data could be compromised, and agencies need to implement Zero Trust controls across these six foundational elements: identities, devices, applications, data, infrastructure, and networks.

dential, and Access Management (ICAM), Security Information and Event Management (SIEM), and Continuous Diagnostics and Mitigation (CDM) tools may already be providing many of the alerts and analysis needed for Zero Trust. The SIEM delivers intelligent security analytics and threat intelligence across the enterprise and provides a single solution for alert detection, threat visibility, proactive hunting, and threat response.

Agencies will also need to incorporate threat intelligence feeds, network and system activity logs, identity management systems, data access policies, and a policy engine. These are all important Zero Trust components. Access to resources will need to be determined by policy and consider the requesting system as well as observable user identity and behavioral traits, and the threat environment. The policy administrator, with its security orchestration automated response solution, acts upon alerts to initiate actions to disconnect offending systems and deny prohibited access to resources. Agencies will need to implement a trusted and secure communications platform between edge devices and services in the cloud or on-premises. A private multi-segment and multi-path blockchain is ideal to securely hold cipher keys and this can be used to enforce the use of enterprise public key infrastructure (PKI).

Thinking about the future, Zero Trust solutions will need to evolve. Quantum computing may be able to crack today's encryption, and artificial intelligence (AI)-powered cyber-attacks may occur. We will certainly need to incorporate AI into Zero Trust implementations and establish a resilient cyber ecosystem through connected technologies like AI. We may need to think about broader implementation of Host Identity Protocol (HIP), or implementation of Blockchain to treat the network as a massive ledger. And we will need continued close cooperation between government and industry. ■

About The Author

Mr. Klimavicz is a Managing Director with KPMG LLP where he leads the government Chief Information Officer (CIO) advisory practice and helps government clients develop and implement digital transformations. Mr. Klimavicz's 37-year career in the federal government began with the Central Intelligence Agency (CIA) as a scientist and culminated with the U.S. Department of Justice (DOJ) as Deputy Assistant Attorney General and CIO from May 2014 until March 2020. Mr. Klimavicz also served as National Oceanic and Atmospheric Administration (NOAA) CIO and Director, High Performance Computing and Communications from 2007 until 2014, and as the National Geospatial-Intelligence Agency Deputy CIO from 2003 to 2007. In 2012, Mr. Klimavicz received the U.S. Presidential Rank Award for Distinguished Executive Service, and he is a CIO-SAGE at the Partnership for Public Service.